N° d'ordre :

N° de série :

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العــالي والبحث العلمـي

جامعة الشهيد حمة لخضر بالــوادي

كلية العلوم والتكنولوجيا

مذكرة التخرج

ليسانس أكاديمي

مجل: الرياضيات و الاعلام الآلي

شعبة الرياضيات

التخصص: نمذجة رياضية و محاكاة عددية

الموضوع

الــتـــــشـــفـــيـــر

مــفـهـومــه و بــعـض أنـظـمـتــه

من إعداد:

- أمان الله سمية
- دو الزهرة
- لشلح الزهرة

الأستاذ المؤطر:

فرحات محمد السعيد

السنة الجامعية 2014 – 2015

شكـــر

سبحان الله و الحمد لله على فضله ونعمه التي لا تعد ولا تحصى، ونسأله أن يجعلنا ممنيطلبون العلم على الوجه الذي يرضيه ونشكره على إلهامنا بالصبر لإتمام هذا العمل المتواضع كما نتقدم بجزيل الشكر إلى:

- ❖ الأستاذ المشرف:فرحات محمد السعيد الذي لم يبخل علينا بتوجيهاته و نصائحه القيمة وإرشاداته الدالة على ودّه و إخلاصه للأمانة العلمية.
- ❖ الأساتذة الذين تعلمنا على أيديهم.
- ❖ إلى كل من كانت له يد العون في إتمام هذا العمل.
- ❖ أعضاء لجنة المناقشة على تفضلهم لمناقشة هذا العمل.

الفصل الأول: عموميات عن التشفير

الفصل الثاني: الموافقات في $\mathbb{Z}$

الفصل الثالث: أنظمة التشفير

a|b	aيقسمb
	مجموعة الأعداد الطبيعية
	مجموعة الأعداد الصحيحة
	مجموعة قواسم العدد a
PGCD (a|b)	**القاسم المشترك الأكبر لـ** a **و** b
a≡b[n]	a **توافق** b **بتردید** n
K =Glm(26)	فضاء المفاتيح
H_1	**المرسل للرسالة المشفرة**
H_2	**المتلقي للرسالة**
E_k	دالة التشفير
D_k	دالة لفك التشفير
P	**فضاء النصوص المشفرة**
K	فضاء المفاتيح
	التطبيق **المطابق**
Σ	**رمز المجموع**
mod	باقي القسمة الصحيحة

مقدمة

تعتبر الكتابة المشفرة أو التشفير بصفة عامة من بين المواضيع التي عرفت قديما وذلك نظرا لحاجة الإنسان إلى حفظ سرية الرسائل و المعطيات المسجلة، حيث يستعمل التشفير في ميادين عدة كالدفاع والأمن و الاقتصاد...الخ

معظم التشفيرات التي ظهرت قديما كانت ضعيفة نوعا ما حيث أمكن اختراقها من طرف المهاجمين مما تطلب تطويرها عبر الزمن، فظهرت عدة أنظمة جديدة متطورة لكل منها صفاته و مميزاته.

وقد قسمت المذكرة إلى ثلاثة فصول، إذ يتناول الفصل الأول عموميات حول التشفير، من أهميته وكيفية عمله موضحين في ذلك الخطوات المتبعة وكذلك سرد أهم علمائه في حين يتناول الفصل الثاني كل التعاريف و الخواص التي تسهل لنا دراسة هذا الموضوع في الموافقات والقسمة في $\mathbb{Z}$ و قد خصصنا في الفصل الثالث دراسة بعض أنظمة التشفير التي تتعلق بالموافقات و القسمة في $\mathbb{Z}$.

ونظرا لما يحمله الموضوع من أهمية علمية و عملية وما يسعه من معلومات غزيرة و متشعبة كذلك ارتأينا أن نقتصر دراستنا على أهم عناصره، ولقلة المراجع فيه خاصة العربية منها التي تكون أكثر وضوحا من المراجع الأجنبية، قمنا بكتابة المذكرة باللغة العربية لتكون مرجعا جديدا يرجع إليه الطلبة و المختصون في الرياضيات.

و في الأخير سنعرض ما توصلنا إليه من خلال خلاصة مختصرة.

الفصل الأول

عموميات عن التشفير

تمهيد:

في هذا الفصل سنركز اهتمامنا على دراسة مفهوم التشفير و كيفية عمله و كذا أنواعه يتم دراسة كل ذلك بالتطرق إلى أنظمة التشفير الكلاسيكية و ما يترتب عنها من موافقات و القسمة الإقليدية في $\mathbb{Z}$

1-1 :مفهوم التشفير:

علم التشفير أو الكتابة المُشفَّرة المسماة بالـ Crytographyهو فن أو علم إخفاء المعلومات بحيث تكون بأمان عند إرسالها أو تخزينها، ويعتبر هذا مجال ذو أهمية كبيرة ، للحكومات التي تستعمله لضمان الأمان والاستقرار لمواطنيها ،وللشركات التي تريد حماية سجلاتها المالية، وأسرارها التجارية، ومعلومات عملائها وموظفيها وغيرها من المعلومات المهمة والخاصة.

ومع ثورة الإنترنت وازدياد مستخدميها ازدادت أهميته للأفراد، فهم يحتاجونه للخصوصية عندما يتعلق الأمر بالمعلومات الشخصية والحساسة، وقد تكون هذه المعلومات رسائل مكتوبة أو محادثات هاتفية أو صوراً أو بيانات تُنقل عبر وسائل الاتصالات الحديثة أو تحفظ وتعالج بواسطة الحواسيب.

ويطلق عليه أحيانا علم التعمية أو علم الكتابة السرية . ومع التقدم السريع والمتنامي لوسائل نقل المعلومات (الاتصالات) ووسائل تخزينها ومعالجتها (الحواسيب) فإنَّ أهمية الرسائل المكتوبة أو البريد بدأت تتضاءل من ناحية، ومن ناحية أخرى ازدادت الحاجة إلى الحفاظ على أمن المعلومات وسريتها.

والتشفير (أو التعمية) هو أهم طرق حماية المعلومات وأكثرها كفاءة خصوصًا إذا كانت المعلومات ستنقل على شبكات اتصال سلكية أو لاسلكية يسهل التصنت عليها، أو كانت المعلومات تتبادل في شبكات الحواسيب الحديثة الواسعة الانتشار التي يمكن اختراقها.

ويعالج هذا العلم مسألتين: تتناول الأولى طرق إخفاء المعلومات المرسَلة من جهة لأخرى وهو ما يسمى بالتعمية أو التشفير ، وتختص الثانية بطرق استخراج المعلومات من قِبَل الملتقط للرسائل المشفّرة، وذلك بدون معرفه المفتاح المتفق عليه بين المتراسلين، وهو ما يسمى كسر الشفرة.

فالمعمِّي أو واضع التعمية يهدف إلى ضمان سرية الرسالة أو إلى ضمان أصالتها وحمايتها من التحريف أو الإدعاء.أما محلل التعمية، فيسعى إلى الهدف المضاد المتمثل في كسر التعمية ومعرفة محتوى الرسالة السرية أو تحريف محتوى الرسالة، أو تزويرها بشكل يؤدي إلى قبولها على أنها رسالة صحيحة أو أصلية وهي غير ذلك. فهدف التعمية هو ضمان سرية الرسالة أو حماية محتوياتها أو مصدرها من التحريف والتزوير، بينما يهدف تحليل التعمية إلى عكس ذلك تماماً.

الأفراد المتخصصون في تطوير وعمل الرموز يطلق عليهم مشفرونCryptographers.أما الأفراد الذين يتخصصون في كسر الرموز وتحليلها فيطلق عليهم محللي التشفيرCryptanalysts.العديد من هؤلاء المحترفين عباقرة ولديهم خلفية قوية في الرياضيات وعلم الحاسبات. هم يعيشون في عالمهم الخاص، و لا يستطيعون أن يتحدثوا عما يعملون.

1-2: نشأة التشفير:

تعتبر الكتابة السرية من أقدم أشكال التشفير فهي قديمة قدم الكتابة نفسها. مع أنّه يجب الإشارة إلى أنّ الكتابة المجرّدة كانت قبل 2000 عام، تمثل بحد ذاتها نوعاً من أنواع الحماية للمعلومات. هذه الكتابة السرية نجدها في هيروغليفية مصر القديمة أو في ألواح من بلاد الرافدين تشرح أسرار الأواني الفخّارية المصقولة.

نشأت خوارزميات التشفير كغيرها من الاكتشافات القديمة في مختلف مجالات النشاط البشري لا يمكن ترتيبها بشكل خطي فهذه الاكتشافات غالبا ما ظهرت في أماكن متفرّقة ولم يكن حينها الاتصال بين مراكز المعرفة المختلفة.حتى أنّه كان السائد التخفي و التكتم على العديد من المعلومات لأنها كانت تقدّم نوعاً من الأفضلية.

كان الإغريق القدماء أفضل من وثّق التشفير في العديد من المجالات العلمية في أوروبا ويرجع ذلك للعديد من الأسباب لكن أهمها هو الانتشار الواسع نسبياً للأبجدية والشكل الكتابي للتعبير منذ القرن الثامن قبل الميلاد.

كيرهوف كان أول من أوضح حقيقة أن أمن خوارزمية التشفير يجب أنَ يعتمد حصراً على إخفاء المفتاح وليس على إخفاء الخوارزمية نفسها. في حين كان هيل من قلَة العلماء الذين كانوا يدركون بأن دخول الرياضيات لمجال التشفير أصبح ضرورة حتمية . فقد استطاع أدرين ألبرت في عام 1941 أن يبني على أعمال هيل الرائدة في هذا المجال حيث أدرك أنَه يمكن استعمال بنى جبرية مختلفة لغرض التشفير.

تطور التشفير موازاة مع تطور تحليل التشفير في مواضيع غيرت مجرى التاريخ و بذلك كانت سبب دخول الولايات المتحدة الحرب العالمية الأولى .

حتى سبعينيات القرن العشرين كان التشفير حكراً على الحكومات، لكن حدثين هامين أديا إلى كسر هذا الاحتكار الحكومي وهما:وضع معيار تشفير البيانات و اختراع التشفير بمفتاح عمومي.

1-3:أهم العلماء:

بدأ استعمال التشفير و الكتابة السرية منذ بدء الحضارة الإنسانية، وقد استخدمه قدماء المصريين وكذلك الإغريق منذ حوالي 1900 سنة قبل الميلاد.

ازدهر هذا العلم عند العرب في القرن الثالث عشر ميلادي، نتيجة لأسباب حضارية و عسكرة و سياسية، وظهرت في تلك الفترة مؤلفات كثيرة في علم التشفير منها: كتاب إبن دنينير "مقاصد الفصول المترجمة عن الترجمة" وكتاب إبن عدلان وكذلك كتاب علي بن الدريهم .

وكان الفيلسوف العربي أبو يوسف يعقوب بن إسحاق الكندي أعظم العلماء العرب في التشفير، ضمت مؤلفاته الكثيرة أول كتاب معروف في علم التشفير "رسالة في استخراج المعمىَ"

و موسوعة عبد الله الكلكشندي بعنوان "صبح الأعشى".

ثم ظهرت بعد ذلك مؤلفات في علم التشفير في أوربا، بترجمات أو اقتباسات مما ترك العرب مع زيادة وتطوير. ثم ظهر هذا العلم قبيل الحرب العالمية الأولى إلى يومنا هذا، ففي عام 1949 م نشر العالم كلود شانون بحثاً مبتكراً عن الاتصالات السرية، و وضع بذلك الأساس الرياضي لعلم التشفير الحديث، وفي عام 1975م ظهر التشفير غير المتناظر. وفي عام 1977م ولأول مرَة في التاريخ تمَ اعتماد الخوارزمية DES في الولايات المتحدة الأمريكية كخوارزمية قياسية لتشفير البيانات.

1-4:كيفية عمل التشفير

يعرف نظام التشفير بخمسة عناصر هي:

- P مجموعة منتهية تمثل فضاء النصوص الواضحة، كل عنصر فيها يسمى رسالة واضحة.
- C مجموعة منتهية تمثل فضاء النصوص المشفرة، كل عنصر فيها يسمى رسالة مشفرة أو كتابة مشفرة.
- K مجموعة منتهية تمثل فضاء المفاتيح، كل عنصر فيها يسمى مفتاح.
- $E = \{E_k, k \in K\}$تمثل عائلة الدوال :$E_k: P \longrightarrow C$ تسمى دوال التشفير،حيث k هو مفتاح منK
- $D = \{D_k, k \in K\}$ تمثل عائلة الدوال: $D_k: C \longrightarrow P$ تسمى دوال فك التشفير.

$$D_k o E_k = id_P \quad \text{بحيث}$$

id_Pهوالتطبيق المطابق من P نحو P .

على سبيل المثال استعمل H_1 نظام التشفير من أجل إرسال رسالة سرية m إلى H_2، فاستعمل H_1 مفتاح التشفير eواستعمل H_2 مفتاح فك التشفير d، ثم قام H_1 بحساب الكتابة المشفرة$c = E\ (m)$ ،وأرسلها إلى H_2الذي أعاد تصميم الرسالة المحسوبة$m = D\ (c)$،والبديهي جدا أن يكون مفتاح فك التشفير السريا.

والصورة التالية توضح كيفية عمل التشفير

مثال توضيحي:

شفرة قيصر من أقدم الشفرات المبتكرة وقد أثبتت فعاليتها في عصره . وفي هذا المثال سنوضح طريقة عمل شفرة قيصر:

إذا شفرنا كلمة"SECRET" و استخدمنا قيمة المفتاح 3 ، فإننا نقوم بتغيير مواضع الحروف ابتداء من الحرف الثالث وهو حرف " D" وعليه فإن ترتيب الحروف سوف يكون على الشكل التالي :

a	b	c	d	e	f	g	h	i	j	k	l	m
n	o	p	q	r	s	t	u	v	w	x	y	z

الحروف بعد استخدام القيمة الجديدة لها من المفتاح "3" يكون على الشكل التالي :

d	e	f	g	h	i	j	k	l	m	n	o	p
q	r	s	t	u	v	w	x	y	z	a	b	c

الآن قيمة الـ Sإلى Vو E إلىH وهكذا .

وبهذا الشكل فإن كلمة "SECRET" سوف تكون : " VHFUHW" لتعطي أي شخص آخر إمكانية قراءة رسالتك المشفرة، ويجب أن ترسل له قيمة المفتاح "3" .

وسوف نتطرق في المبحث الأخير إلى أنواع أخرى من أنظمة التشفير وخاصة التي تتعلق بالموافقات والقسمة الإقليدية في ℤ.

1-5:أنواع التشفير

1-5-1:التشفير المتماثل(المتناظر):

في التشفير المتماثِل، يستخدم+ كل من المرسِل والمستقبِل المفتاح السري ذاته في تشفير الرسالة وفك تشفيرها.ويتفق الطرفان في البداية على عبارة المرور

pass phrase (كلمات مرور طويلة) التي سيتم استخدامها. ويمكن أن تحوي عبارة المرور حروفاً كبيرة وصغيرة ورموزا أخرى. وبعد ذلك، تحوِّل برمجيات التشفير عبارةَ المرور إلى عدد ثنائي، ويتم إضافة رموز أخرى لزيادة طولها. ويشكل العدد الثنائي الناتج مفتاح تشفير الرسالة.

و يستخدم المستقبِل عبارةَ المرور نفسها من أجل فك شفرة و بعد استقبال الرسالة المُشَّفرة.

(cipher text encrypted or text)، إذ تترِجم البرمجيات مرة أخرى عبارةَ المرور لتشكيل المفتاح الثنائي (binary Kay)الذي يتولى إعادة تحويل النص المُشَّفر إلى شكله الأصلي المفهوم.

ويعتمد مفهوم التشفير المتماثِل على معيار DES(Standard Encryption Data). أما الثغرة الكبيرة في هذاالنوع من التشفير فتكمن في تبادُل المفتاح السري دون أمان، مما أدى إلى تراجع استخدام هذا النوع من التشفير، ليصبح شيئاً من الماضي. والصورة التالية توضح التشفير المتناظر.

صورة توضيحية للتشفير المتناظر

1-5-2:التشفير غير المتماثل (غير المتناظر):

جاء التشفير غير المتماثل حلاً لمشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل، فعوضاً عن استخدام مفتاح واحد، يستخدم التشفير غير المتماثل مفتاحين اثنين تربط بينهما علاقة. ويُدعى هذان المفتاحان بالمفتاح العام (Public Key) والمفتاح الخاص(Private key).

ويكون المفتاح الخاص معروفاً لدى جهة واحدة فقط أو شخص واحد فقط؛ وهو المرسِل، ويُستخَدم لتشفير الرسالة وفكها. أما المفتاح العام فيكون معروفاً لدى أكثر من شخص أو جهة، ويستطيع المفتاح العام فكشفرة الرسالة التي شَّفرها المفتاح الخاص، ويمكن استخدامه أيضاً لتشفير رسائل مالك المفتاح الخاص،

ولكن ليس بإمكان أحد استخدام المفتاح العام لفك شفرة رسالة شفَّرها هذا المفتاح العام، إذ إن مالك المفتاح الخاص هو الوحيد الذي يستطيع فك شفرة الرسائل التي شفرها المفتاح العام.

ويُدعى نظام التشفير الذي يستخدم المفاتيح العامة بنظام Reive ,Aselmen et Shair ,Reivest (RSA)، ورغم أنه أفضل وأكثر أمناً من نظام DES إلا إنه أبطأ؛ إذ إن جلسة التشفير وجلسة فك التشفير يجب أن تكونا متزامنتين تقريبا.

والصورة التالية توضح التشفير غير المتناظر

صورة توضيحية للتشفير غير المتناظر

1-6 :أهمية التشفير واستخداماته:

اكتسب علم التشفير وتطبيقاته أهمية بالغة منذ مطلع القرن العشرين ،ففي منتصف السبعينات استعمال التشفير تعدّى الاتصالات والمراسلات العسكرية والدبلوماسية والأمنية ووصل إلى عدة مجالات وتطبيقات واستخدامات منها:

- في الصناعة والتجارة للمحافظة على الأسرار التجارية والعلمية والاختراعات والتصميمات والوضع المالي للمؤسسات وغيرها.

- في البث المرئي حيث يتم تشفير القنوات المرئية حتى لا يستطيع مشاهدتها إلا المشتركون الذين يدفعون اشتراكا شهريا مقابل المفتاح السري الذي يسمح بفك تشفير القنوات ومشاهدة البرامج.

- في المصارف للمحافظة على حسابات الزبائن وحمايتها من التلاعب

أو الاختلاس خصوصا مع تطور الخدمات المصرفية الإلكترونية.

- في شبكات الحواسيب والحواسيب الشخصية للمحافظة على المعلومات الحساسة وحماية الملفات، وحماية الدخول إلى الشبكات عن طريق كلمة المرور الخاصة بكل مستخدم .

- في حماية الاتصالات السلكية واللاسلكية وهواتف السيارات من الالتقاط والتصنت والإطلاع على أسرار الآخرين الشخصية والعائلية.

- الكشف عن اللغات القديمة البائدة حيث كان لعلم تحليل التشفير أكبر الأثر في الكشف عن الرموز اللغة الهيروغليفية في مطلع القرن التاسع عشر.

الفصل الثاني

الموافقات في $\mathbb{Z}$

تمهيد:

في الفصل الأول تعرفنا على مفهوم التشفير و أنواعه و طرقه ، وفي هذا الفصل سندرس القسمة الاقليدية والموافقات في $\mathbb{Z}$ ، لأهميتها في الكثير من أنظمة التشفير الكلاسيكية كالتشفير التآلفي.

2-1: قابلية القسمة في $\mathbb{Z}$

2-1-1: تعريف

a و b عددان صحيحان و a غير معدوم.

نقول أن العدد a يقسم العدد b يكافئ وجود عدد صحيح k حيث: $b=ka$.

نقول كذلك a قاسم للعدد b أو b مضاعف للعدد a.

نكتب $a|b$ و نقرأ a يقسم b.

أمثلة:

$6 \times 8 = 48$ ومنه $6|48$.

$(-6) \times (-8) = 48$ ومنه $(-6)|48$.

$5 \times (-13) = (-65)$ ومنه $5|(-65)$.

$5 \times (-13) = (-65)$ ومنه $(-13)|(-65)$.

2-1-2: خواص:

خاصية1:

a، b، c ثلاثة أعداد صحيحة غير معدومة.

إذا كان a يقسم b و b يقسم c فإن a يقسم c.

البرهان:

إذا كان $a|b$ و $b|c$ فإن $b= ka$ و $c= kb$ حيث k و k' عددان صحيحان ومنه $c=(kk')\ a$

وبما أن kk' عدد صحيح فإن a يقسم c.

خاصية2:

a وb عددان صحيحان و a غير معدوم.

إذا كان a يقسم b فإنه من أجل كل عدد صحيح m، a يقسم mb.

البرهان:

إذا كان $a|b$ فإن $b= ka$ حيث k عدد صحيح ومنه $mb = mkb = (mk)a$

وبما أن mk عددا صحيحا فإن a يقسم mb.

خاصية3:

a وb عددان صحيحان و a غير معدوم.

إذا كان $a|b$ و m عدد صحيح غير معدوم فإن ma يقسم mb.

البرهان:

إذا كان $a|b$ فإن $b=ka$ حيث k عدد صحيح ومنه $mb = mka = k(ma)$

وبما أن k عدد صحيح فإن ma يقسم mb.

خاصية4 :

a، b و c ثلاثة أعداد صحيحة وa غير معدوم.

إذا كان a يقسم العددين b و c هذا يكافئ من أجل كل عددين صحيحين m و n:

a يقسم $mb + nc$.

البرهان:

إذا كان a|b و a|c فإن b=ka و c=k'a حيث k و 'k عددان صحيحان و منه:mb+nc=mka+nk'a .

.mb+nc=(mk+nk')a

بما أن 'mk+nk عدد صحيح فإن a يقسم mb+nc.

2-2: القسمة الإقليدية في $\mathbb{Z}$

2-2-1: مبرهنة

a عدد صحيح و b عدد طبيعي غير معدوم.

توجد ثنائية وحيدة (q,r) من الأعداد الصحيحة حيث a= bq+ r و $0\leq r< b$.

تسمى عملية البحث عن الثنائية (q,r) بالقسمة الإقليدية للعدد a على العدد b.

يسمى q و r بهذا الترتيب حاصل و باقي القسمة الإقليدية للعدد a على العدد b.

البرهان:

العدد a إما مضاعف لـ b وإما محصور بين مضاعفين متتابعين لـ b أي يوجد عدد صحيح وحيد حيث $qb\leq$ a< (q+1) ونستنتج من هذا أن $0\leq a- qb< b$.

نضع r= a− qb و منه لدينا a= bq+ r مع $0\leq r< b$.

ملاحظة:

يمكن تمديد مفهوم القسمة الإقليدية لعدد صحيح a على عدد صحيح غير معدوم b.

ونحصل على a= bq+ r و $0\leq r< |b|$.

2-3: القاسم المشترك الأكبر لعددين طبيعيين

a عدد طبيعي غير معدوم. نرمز بـ D_a إلى مجموعة قواسم العدد a.

مثال:

1. مجموعة قواسم 8 هي $D_8 = \{1;2;4;8\}$.
2. مجموعة قواسم 0 هي $\mathbb{N}^*$.

2-3-1: تعريف

a و b عددان طبيعيان غير معدومين.

D_a و D_b مجموعتا قواسم a و b على الترتيب.

$D_a \cap D_b$ هي مجموعة القواسم المشتركة للعددين a و b.

يسمى أكبر عنصر من المجموعة $D_a \cap D_b$ بالقاسم المشترك الأكبر للعددين a و b.

ونرمز له بـ PGCD(a;b).

2-3-2: ملاحظات

1. PGCD(a;a)=a و PGCD(1;a)=1.
2. PGCD(0;a)=a (a غير معدوم).
3. مجموعة القواسم المشتركة لعددين طبيعيين غير معدومين هي مجموعة قواسم قاسمهما المشترك الأكبر.
4. يكون العددان a و b أوليين فيما بينهما إذا وفقط إذا كان قاسمهما المشترك الأكبر يساوي 1.
5. يمكن تمديد القاسم المشترك الأكبر لعددين صحيحين غير معدومين a و b بكونه العدد الوحيد d حيث: d= PGCD(|a|;|b|)

مثال:

ليكن n عددا صحيحا.

وليكن العددان الصحيحان $a= 5n- 2$ و $b= 2n+ 3$.

أثبت أن كل قاسم مشتركا للعددين a و b يقسم العدد 19.

الحل:

ليكن d قاسما مشتركا للعددين a و b.

ومنه d يقسم $2a- 5b$ أي d يقسم $(5n- 2)\times 2-(2n+ 3)\times 5$ أي d يقسم 19.

مبرهنة:

a و b عددان طبيعيان غير معدومين حيث $a\geq b$.

r باقي قسمة a و b. $PGCD(a;b)= PGCD(b;r)$

البرهان:

نضع $PGCD(a;b)= d$ و $PGCD(b;r)= d'$.

نعلم أن $a= bq+ r$ حيث q عدد طبيعي. ومنه $r= a- bq$.

d يقسم b وبالتالي d يقسم bq و d يقسم a إذن d يقسم $a- bq$ أي d يقسم r.

ومنه d قاسم مشترك للعددين b و r.

'd يقسم b وبالتالي 'd يقسم bq و 'd يقسم r إذن 'd يقسم $bq+ r$ أي 'd يقسم a.

ومنه 'd قاسم مشترك للعددين a و b.

إذن مجموعة القواسم المشتركة للعددين a و b هي نفسها مجموعة القواسم المشتركة للعددين b و r.

بالتالي d= d' أي PGCD(a;b)= PGCD(b;r).

2-3-3: خوارزمية إقليدس

a و b عددان طبيعيان غير معدومين حيث a> b.

بقسمة a على b نحصل على $a= bq_1+ r_1$ و $a\leq r_1<b$ حيث q_1 و r_1 عددان طبيعيان .

- إذا كان $r_1= 0$ (اي b يقسم a) فإن PGCD(a;b)= b.
- إذا كان $r_1\neq 0$ فإن $PGCD(a;b)= PGCD(b;r_1)$. نقسم b على r_1 نحصل على $b= r_1q_2+ r_2$ حيث q_2 و r_2 عددان طبيعيان.
- إذا كان $r_2= 0$ (r_1اي b يقسم) فإن $PGCD(a,b)= PGCD(b; r_1)= r_1$.
- إذا كان $r_2\neq 0$ فإن $PGCD(a;b)= PGCD(b; r_1)= PGCD(r_1; r_2)$.

نقسم r_1 على r_2 نحصل على $r_1= r_2q_3+ r_3$ و $0\leq r_3< r_2$ حيث q_3 و r_3 عددان طبيعيان.

- نواصل هكذا حتى نجد باقيا معدوما. ونسمي r_n آخر باقي غير معدوم وعليه:

$$PGCD(a;b)= PGCD(b; r_1)=PGCD(r_1; r_2)=\ldots=PGCD(r_n; 0)=r_n$$

هذه الطريقة لإيجاد القاسم المشترك الأكبر لعددين طبيعيين تسمى

خوارزمية إقليدس.

مثال:

تعيين PGCD(1631; 932).

$1631= 932\times 1+ 699$.

$932= 699\times 1+ 233$.

$699= 233\times 3+ 0$.

ومنه: $PGCD(1631; 932)= 233$.

2-3-4: خواص

خاصية1:

a و b عددان طبيعيان عير معدومين.

k عدد طبيعي غير معدوم.

$PGCD(ka;kb)=k\times PGCD(a;b)$

البرهان:

نضع $PGCD(a;b)=d$ و $PGCD(ka;kb)=d'$.

d و d' عددان طبيعيان غير معدومين.

d يقسم a ومنه kd يقسم ka.

d يقسم b ومنه kb يقسم kd و بالتالي kd قاسم مشترك للعددين ka و kb إذن kd يقسم القاسم المشترك الأكبر للعددين ka و kb أي kd يقسم d' ومنه يمكن كتابة $d'= k' (kd)$ حيث k' عدد طبيعي.

كذلك d' يقسم ka و kb.

ومنه k'kd يقسم ka و kb و بالتالي k'd يقسم a و b و بالتالي k'd يقسم القاسم المشترك الأكبر للعددين a و b وبالتالي $k'= 1$. ومنه $d'= kd$.

إذن $PGCD(ka;kb)= k\times PGCD(a;b)$.

خاصية2:

a و b عددان طبيعيان غير معدومين.

d قاسم مشترك للعددين a و b.

نضع $a= da'$ و $b= db'$.

يكون d القاسم المشترك الأكبر للعددين a و b إذا وفقط إذا كان العددان الطبيعيان 'a و 'b أوليان فيما بينهما.

البرهان:

a و b عددان طبيعيان غير معدومين و d قاسمهما المشترك الأكبر.

- نضع $a= da'$ و $b= db'$

$$d= PGCD(a;b)= PGCD(da';db')$$

$$= d\times PGCD(a';b')$$

بما ن d غير معدوم فإن : $PGCD(a';b')= 1$.

- المسألة العكسية. نعتبر $PGCD(a;b)= d\times PGCD(a';b')= d$.

مثال:

عين كل الثنائيات $(a;b)$ من الأعداد الطبيعية غير المعدومة حيث:

$$\begin{cases} a + b = 66 \\ PGCD(a; b) = 6 \end{cases}$$

الحل:

نضع $a=6a'$ و $b=6b'$ حيث 'a و 'b عددان أوليان فيما بينهما.

$a+b=66$ تعني $6a'+ 6b'=66$ و منه $a'+ b'=11$

$$(a;b)\epsilon\{(1;10),(2;9),(3;8),(4;7),(5;6),(6;5),(7;4),(8;3),(9;2),(10;1)\}$$

ومنه مجموعة الحلول $(a;b)$ هي:

$$\{(6;60),(12;54),(18;48),(24;42),(30;36),$$

$$(36;30),(42;24),(48;18),(54;12),(10;1)\}$$

خاصية3:

a و b عددان صحيحان غير معدومين. k عدد صحيح غير معدوم.

.PGCD(ka;kb)= |k|PGCD(a;b)

2-4:الموافقات في $\mathbb{Z}$

2-4-1:تعريف

a و b عددان صحيحان، n عدد طبيعي و يختلف عن 1.

نقول إن a و b متوافقان بتردید n إذا و فقط إذا كان n يقسم a−b أي a−b مضاعف للعدد n. اصطلاحا نكتب: a≡b[n] و نقرأ a يوافق b بتردید n.

مثال:

18−6=12=4×3 لأن 10≡ 6[4].

كذلك −6≡10[4] لأن −6−10= −16=4(−4).

2-4-2: نتائج

1) a≡ 0[n] يكافئ n قاسما للعدد a.
2) إذا كان a≡ r[n] و 0≤ r<n، إذن r هو باقي القسمة الإقليدية للعدد a على n.
   مثل: 23≡ 3[20] حيث r= 3 و 0≤ 3< 20.

2-4-3: <u>خواص</u>

n عدد طبيعي غير معدوم و يختلف عن 1.

<u>خاصية1</u>:

من أجل كل عدد صحيح a فإن: a≡ a[n].

وهذا واضح لكون a= 0 −a، و 0 مضاعف n.

خاصية2:

من أجل a، b في $\mathbb{Z}$ و n في $\mathbb{N}^*$ مع $n\geq 2$.

$a\equiv b[n]$ يكافئ $b\equiv a[n]$.

خاصية3:

من أجل كل عدد من الأعداد الصحيحة: a، b، c فإن:

إذا كان: $a\equiv b[n]$ و $b\equiv c[n]$ فإن: $a\equiv c[n]$.

البرهان:

بما أن $a\equiv b[n]$ و $b\equiv c[n]$ فإن: $a-b$ و $b-c$ مضاعفات للعدد n و عليه يوجد عددان صحيحان p و q بحيث: $a-b=pn$ و $b-c=qn$ و بالجمع نجد: $a-c=(p+q)n$ و عليه:

$(a-c)$مضاعف n إذن: $a\equiv c[n]$.

خاصية4:

من أجل كل عدد من الأعداد الصحيحة: a، b، x، y حيث:

إذا كان: $a\equiv b[n]$ و $x\equiv y[n]$ فإن: $a+x\equiv b+y[n]$.

خاصية5:

من أجل كل عدد من الأعداد الصحيحة: a، b، x حيث:

إذا كان: $a\equiv b[n]$ فإن: $a+x=b+x[n]$.

البرهان:

لدينا: $a\equiv b[n]$ و $x\equiv x[n]$ من الخاصية 1.

و حسب الخاصية 4 فإن: $a+x=b+x[n]$.

خاصية6:

من أجل كل عدد من الأعداد الصحيحة: a، b، x، y حيث:

إذا كان: $a\equiv b[n]$ و $x\equiv y[n]$ فإن: $a.x\equiv b.y[n]$.

البرهان:

بما أن: $a \equiv b[n]$ و $x \equiv y[n]$ فإنه يوجد عددان صحيحان p و q بحيث: $a - b = p.n$ و $x - y = q.n$.

و لدينا: $ax - by = ax - bx + bx - by$

و منه: $ax - by = (a - b)x + (x - y)b$

$= qnx + pnb$

$= (qx + pb)n$

وعليه: $ax - by$ مضاعف n إذن: $ax \equiv by[n]$.

خاصية7:

من أجل كل عدد من الأعداد الصحيحة: a، b، x حيث:

إذا كان: $a \equiv b[n]$ فإن: $xa \equiv xb[n]$.

البرهان:

لدينا: $a \equiv b[n]$ و $x \equiv x[n]$ حسب الخاصية 1.

و عليه: حسب الخاصية 6 فإن $xa \equiv xb[n]$.

خاصية8:

من أجل كل عددين صحيحين a و b و من أجل كل عدد طبيعي غير معدوم λ.

إذا كان: $a \equiv b[n]$ فإن: $\lambda a \equiv \lambda b[\lambda n]$.

البرهان:

لدينا: $a \equiv b[n]$ و منه يوجد عدد صحيح p حيث: $a - b = pn$.

وعليه: $\lambda(a - b) = \lambda pn$ أي: $\lambda a - \lambda b = p(\lambda n)$

ومنه: $\lambda a - \lambda b$ مضاعف للعدد λn و بالتالي: $\lambda a \equiv \lambda b[\lambda n]$.

خاصية9:

من أجل كل عددين صحيحين a و b و من أجل كل عدد طبيعي غير معدوم p.

إذا كان: $a \equiv b[n]$ فإن: $a^p \equiv b^p[n]$.

البرهان:

- من أجل p= 1: إذا كان $a\equiv b[n]$ فإن: $a^1\equiv b^1[n]$ و هذا صحيح وعليه بداية التراجع صحيحة.
- نفرض صحة الخاصية من أجل k و نبرهن صحتها من أجل k+1 أي نفرض أنه: إذا كان: $a\equiv b[n]$ فإن: $a^k\equiv b^k[n]$ و نبرهن أنه:

إذا كان: $a\equiv b[n]$ فإن: $a^{k+1}\equiv b^{k+1}[n]$

إذا كان $a\equiv b[n]$ فإن: $a^k\equiv b^k[n]$ صحيحة.

و حسب الخاصية 6: $a^k.a\equiv b^k.b[n]$

وعليه: $a^{k+1}\equiv b^{k+1}[n]$ إذن الخاصية وراثية.

و منه الخاصية صحيحة من أجل كل عدد طبيعي غير معدوم p.

مثال:

1. ادرس بواقي قسمة 2^n على 7. ثم استنتج باقي قسمة 2^{1962} على 7.
2. أثبت أن العدد: $2^{3n+1}+2^{12n}+10$. 12 يقبل القسمة على 7 من أجل كل عدد طبيعي n.

الحل:

1. بواقي قسمة 2^n على 7:

$2^0\equiv 1[7]$;$2^1\equiv 2[7]$; $2^2\equiv 4[7]$; $2^3\equiv 1[7]$

ومنه من العلاقة $2^3\equiv 1[7]$ وحسب الخاصية 9 لدينا:

$2^{3p}\equiv 1[7]$ من أجل كل عدد طبيعي p.

ليكن: $2\equiv 2[7]$ و عليه: $2^{3p}.2\equiv 1.2[7]$ إذن: $2^{3p+1}\equiv 2[7]$

وكذلك: $2^2\equiv 4[7]$ و عليه: $2^{3p}.2^2\equiv 1.4[7]$

إذن: $2^{3p+2}\equiv 4[7]$

و بالتالي لما: n= 3p: $2^n\equiv 1[7]$

و لما: n= 3p+ 1: $2^n\equiv 2[7]$

و لما: n= 3p+ 2: $2^n\equiv 4[7]$

استنتاج باقي قسمة 2^{1962} على 7:

لدينا: $1962= 3\times 654$ ومنه: $1962= 3p$

ومنه: $2^{1962}\equiv 1[7]$

2. إثبات أن: $12.2^{3n+1}+ 10.2^{12n}+ 8\equiv 0[7]$

لدينا: $12\equiv 5[7]$ و $2^{3n+1}\equiv 2[7]$

وعليه: $12.2^{3n+1}\equiv 2\times 5[7]$

إذن: $12.2^{3n+1}\equiv 3[7]$ ...(1) لأن: $10\equiv 3[7]$

و لدينا: $2^{12n}=(2^{3n})^4$ و عليه و بما أن: $2^{3n}\equiv 1[7]$

فإن: $(2^{3n})^4\equiv (1)^4[7]$ أي: $2^{12n}\equiv 1[7]$ ...(2)

و عليه من (1) و (2) نجد: $12.2^{3n+1}+ 2^{12n}+ 10\equiv 4+10[7]$

إذن: $12.2^{3n+1}+ 2^{12n}+ 10\equiv 0[7]$

الفصل الثالث

أنظمة التشفير

تمهيد:

في الفصل الثاني تعرضنا إلى بعض خواص الموافقات و القسمة في $\mathbb{Z}$، كما قمنا بتقديم أمثلة عليها أما في هذا الفصل سنقوم بتطبيق مجموعة من تلك التعاريف و الخواص في دراسة بعض أهم نماذج التشفير الكلاسكية التي تندرج ضمن حلقة الأعداد الصحيحة $\mathbb{Z}$ لأهميتها في نسج أنظمة التشفير.

3-1-التشفير بالطرق الكلاسيكية Calassicalmethodecipher

سنعرض في مايلي بعض الأمثلة عن التشفيرات الكلاسيكية حيث يرمز للحروف الأبجدية الستة و العشرين بأرقام من الزمرة $\mathbb{Z}_{26}=\frac{\mathbb{Z}}{26\mathbb{Z}}$.

3-1-1- التشفير بالتعويض cipherSubstitution

$\mathbb{Z}_{26}$ = C = P وفضاء المفاتيح هو زمرة تبديلات $\mathbb{Z}_{26}$.

من أجل $k \in$ K لدينا $e_k=k$ و $d_k = k^{-1}$.

مثال تطبيقي:

لدينا التبديلة التالية:

1	2	3	4	5	6	7	8	9	10	11	12	13
a	b	c	d	e	f	g	h	i	j	k	l	m
p	o	m	l	i	k	u	j	n	y	h	b	t

13	14	15	16	17	18	19	20	21	22	23	24	25
n	o	p	q	r	s	t	u	v	w	x	y	z
g	r	f	v	d	c	e	z	s	x	a	q	W

هي تقابل من $\mathbb{Z}_{26}$ نحو $\mathbb{Z}_{26}$.

فالنص mat يشفر إلى tpe حيث نلاحظ أن الحرفm يقابله الحرف t في هذه التبديلة، ونفس الطريقة نطبقها على بقية الأحرف.

3-1-2- التشفير بالإزاحة cipherDisplacement

لدينا $E = K = \mathbb{Z}_{26}$ =P و $b_K(x) = x+k$ كذلك $D_k(y) = ky -$ و $Kk \in$ كحالة خاصة

من أجل $k = 3$، النص الواضح هو bienveu يشفر إلى elhqyhqx.

مثلا: لنأخذ الحرفbيقابل الرتبة 1 فهو يشفر كالتالي:

$$E_3(b) = E_3(1) = 1+3 = 4$$

و 4 يقابله الحرف e، إذن الحرف b يشفر الى الحرف e.

كذلك لو أردنا تشفير الحرف x فهو يقابل الرتبة 25 و بالتالي:

$$E_3(x) = E_3(25) = 3 + 25 = 28 = 2+26 = 2$$

وهذا لأن الأحرف الأبجدية المستعملة موجودة ضمن الزمرة $\mathbb{Z}_{26}$.

ملاحظة:

إن نظام التشفير هذا غير آمن لأنه يمكن تجربة كل المفاتيح حتى يتم الحصول على المفتاح المناسب لفك التشفير.

3-1-3- تشفير هيل Hill cipher

$P = C = \mathbb{Z}_{26}^m$ حيث $\mathbb{N}^* m$، و فضاء المفاتيح هو $K = Gl_m(\mathbb{Z}_{26})$ هي الزمرة المتكونة من المصفوفات المربعة m × m القابلة للقلب ذات المعاملات في $\mathbb{Z}_{26}$.

ومن أجل $k \epsilon K$لدينا:

$$E_k(x_1, \ldots, x_m) = (x_1, \ldots, x_m)k$$

$$D_k(y_1, \ldots, y_m) = (y_1, \ldots, y_m)k^{-1}$$

مثال تطبيقي:

علينا أولا إختيار المفتاح، مثلا إذا كان مكون من تسعة حروف سوف تكون المصفوفة (الخاصة بالمفتاح) 3×3.

لدينا جملة التشفير التالية: gybnqkurp.

بعد إعطاء كل حرف قيمته، نقوم بوضعه داخل المصفوفة على شكل(3×3) و يكون شكل المصفوفة كالتالي:

وليكن النص الأصلي هوact وفي حالة يكون أكبر من ذلك يتم تقسيمه إلى بلوكات، كل بلوك يتكون من ثلاثة أحرف.

نقوم بوضع النص الأصلي داخل مصفوفة(3×1).

الآن نقوم بضرب المصفوفتين ونأخذ الناتج بعملية باقي القسمة على 26.

$$\begin{pmatrix}6 & 24 & 1\\13 & 16 & 10\\20 & 17 & 15\end{pmatrix}\begin{pmatrix}0\\2\\19\end{pmatrix}\equiv\begin{pmatrix}67\\222\\319\end{pmatrix}\equiv\begin{pmatrix}15\\14\\7\end{pmatrix}\bmod 26$$

اذن الناتج بعد تحويل الأرقام إلى حروف (بمساعدة جدول الحروف) أي النص المشفرهو poh.

كسر الشفرة:

لفك التشفير كل ماعلينا هو إيجاد معكوس المصفوفة، ونقوم بضربه في النص المشفرمع أخذ باقي القسمة على 26 كما هو موضح:

$$\begin{pmatrix}8 & 5 & 10\\12 & 8 & 21\\21 & 12 & 8\end{pmatrix}\begin{pmatrix}15\\14\\7\end{pmatrix}\equiv\begin{pmatrix}260\\574\\539\end{pmatrix}\equiv\begin{pmatrix}0\\2\\19\end{pmatrix}\bmod 26$$

ملاحظة:

هناك أنواع كثيرة من هذه الشفرات منها 3−hill chiffre في هذه الحالة يجب أن تكون المصفوفة (3×3)مثل المثال المدروس سابقا، وفي حالة النوع 2−hill chiffre يجبأن تكون (2×2) وبشكل عام إذا كانت لدينا شفرة n−hill chiffre فإن نوع المصفوفة يكون (n×n).

3−1−4−التشفير التآلفي Affine cipher

ليكنm عدد صحيح موجب، التشفير التآلفي والأبجدية $\mathbb{Z}_m = \frac{\mathbb{Z}}{m\mathbb{Z}}$ هوتشفير بواسطة خانة طولها n = 1.

إن فضاء المفاتيح يتالف من جميع الأزواج $\mathbb{Z}_m^2 \epsilon (a; b)$ حيث aأولي مع m.

1. دالة التشفير E_kهو التطبيق المعرف كمايلي:

$$E_k : \Sigma \to \Sigma$$

$$x \mapsto (a\,x + b) \bmod m$$

2. دالة فك التشفير $\mathcal{D}_k$ هو التطبيق المعرف كمايلي:

$$\mathcal{D}_k : \Sigma \to \Sigma$$

$$x \mapsto a'(x - b) \bmod m$$

لحساب مفتاح فك التشفير المقابلة لمفتاح التشفير (b ، a) نحل التطابق $aa' \equiv 1 \bmod m$ مع الخوارزمية الإقليدية الموسعة وهذا المفتاح هو (a' ، b).

مثال:

إذا إختار H_1:

m = 26 و(3 ، 7)= (a ، b)

ويشفر كلمة التشفير bald (أصلع) بالتشفير التآلفي فيحصل على:

b	A	L	d
1	0	11	3
10	3	5	24
k	D	F	y

H_2 يحسب فك التشفير المقابل، فإنه يحدد عدد صحيح 'a مع $7a' \equiv 1 \bmod 26$ و حسب الخوارزمية الإقليدية الموسعة تعطى 15 = 'a، وبالتالي وظيفة فك التشفير يستبدل الرمز σ
له بـ $15(\sigma - 3) \bmod 26$ وهكذا يحسب H_2.

k	D	F	y
10	3	5	24
1	0	11	3
b	A	L	d

يستمر فضاء المفاتيح لتشفير تآلفي في الحالة 26= m بـ 312 = 26 × φ (26) عنصرا.
حيث يمكن كسر الشفرات التآلفية من قبل حساب سهل على الجبر الخطي، كما أن المهاجم يكفيه معرفة حرفين فقط لإيجاد مفتاح التشفير، كما هو موضح في المثال التالي:

مثال:

يتم إستبدال الأبجدية $\{a; b; \dots; z\}$ بـ $\mathbb{Z}_{26}$ بالطريقة المعتادة في السابق، إذاكان H_1 يستعمل تشفير تآلفي بمفتاح ثابت (a; b)،مثلا إذا عرفنا أن H_1 يشفر e الى r و s الى h، فإننا نستنتج التطبيقات التالية:

$$4a + b \equiv 17 \bmod 26 \dots(1) \quad \text{و} \quad 18a + b \equiv 7 \bmod 26 \dots(2)$$

من(1) نجد: $b \equiv 17 - 4a \bmod 26$

وبالتعويض في (2) نحصل على:

$$18a + 17 - 4a \equiv 7 \bmod 26$$

مما يعني $14a \equiv 16 \bmod 26$

ونستنتج أن $7a \equiv 8 \bmod 13$

بالضرب في (2) نجد: $14a \equiv 16 \bmod 13$ و نحصل على $a \equiv 3 \bmod 13$

مما يسمح لنا بحساب $a = 3$ و $b = 5$.

3-1-5-تشفير أتباش Atbashcipher

هذا الشفرة أيضا من أبسط أنواع الشفرات، وهي كانت في الأصل للغة العبرية، ولكن يمكن إستخدام المفهوم إلى باقي اللغات.

الطريقة:

وهي أن نجعل الحرف الأول في اللغة هو الحرف الأخير، والحرف الثاني ماقبل الأخير وهكذا كما هو موضح في الجدول التالي:

a	b	c	d	e	f	g	h	i	j	k	l	m
z	y	x	w	v	u	t	s	r	q	p	o	n

n	o	p	q	r	s	t	u	v	w	x	y	z
m	l	k	j	i	h	g	f	e	d	c	b	a

مثلا:

تشفير كلمة money الى nlmvb.

ملاحظة:

في بعض الأحيان من الممكن أن تكون الكلمات بعد التشفير يكون لديها معنى وهي مشفرة.

مثال:

الكلمة	hod	hold	Holy	Slim	rip	old	told	tilt
تشفيرها	slw	slow	Slob	Horn	irk	how	glw	grog

ومع ذلك تبقى تلك الشفرات من أسهل الأنواع على الإطلاق.

3-1-6- تشفير سيزار Cesarcipher

الثلاثية المتمثلة في فضاء الرسائل الواضحة والرسائل المشفرة كذلك المفاتيح تكون ضمن المجموعة :

Σ = a{ ، b ، ... ، z }

مثلا:

في الجدول الآتي نقوم بمطابقة الأحرف a ،b ،...،z مع الأرقام 25 ، ....، 0،1،2 هذا ما يسمح بتعيين الأحرف بالأرقام.

0	1	2	3	4	5	6	7	8	9	10	11	12
a	b	c	d	e	F	g	h	i	j	k	l	m
13	14	15	16	17	18	19	20	21	22	23	24	25
n	o	p	q	r	S	t	u	v	w	x	y	z

1. دالة التشفير E مرتبطة بالمفتاح $e \in \mathbb{Z}_{26}$، وتكون معرفة كالتالي:

$$E_e: \Sigma \longrightarrow \Sigma$$

$$x \longmapsto (x + e) \mod 26$$

2. دالة فك التشفير E مرتبطة بالمفتاح $d \in \mathbb{Z}_{26}$ ، وتكون معرفة كالتالي:

$$\mathcal{T} : \Sigma \longrightarrow \Sigma$$
$$x \longmapsto (x + e) \mod 26$$

حيث مفتاح فك التشفير d يناظر مفتاح التشفير e اي e = d.

ملاحظة:

المساواة بين المفاتيح ليس قاعدة عامة في أنظمة التشفير لإيجاد الكتابة المشفرة.

مثال تطبيقي:

من أجل e = 5 النص الواضح cryptographie يشفر إلى hwduytlwfumnj وذلك

مثلا:الحرف r تقابله الرتبة 17 وهو يشفر رقميا كالآتي:

$$E_e(r) = E_5(17) = 17+5 = 22$$

حيث الرتبة 22 يقابلها الحرفw، إذن الحرف r يشفر إلى الحرف w، وبنفس الطريقة تشفر بقية الأحرف.

ملاحظة:

يمكن القول عن تشفير سيزار أنه غير آمن، وذلك لسهولة إيجاد الكتابة الواضحة إنطلاقا من الكتابة المشفرة، وذلك بتجريب كل المفاتيح حيث لا نحتفظ إلا بالكتابة ذات المعنى، و بالتالي نجد الرسالة

و المفتاح الذي تم إستخدامه.

3-1-7-تشفير ROT13

تعتبر هذه الشفرة ضعيفة للغاية حيث أن التشفير وفك التشفير يتم بنفس الطريقة، ومفتاح التشفير هو 13 و للتشفير نقوم بجمع 13 على الحرف الأول من النص الأصلي.

$$P = ROT13(ROT13(P))$$

p: يمثل الحرف الأول من النص الأصلي plaintext.

مثال:

كلمة dollr

لدينا الحرف الأول من النص الأصلي هو d، الحرف d ذو الرتبة 3 نقوم بـ:

$$(13+3) \bmod 26 = 16$$

أو نتحرك ب 13 خطوة من الحرف d و الناتج هو q سواء بالتحريك أو الجمع.

وبنفس الطريقة :

o تشفر إلى حرف b ، الحرف L إلى y ، والحرف r إلى e

فك التشفير:

مثلا لدينا الحرف q ونقوم بفك التشفير كالتالي:

$$(16+13) \bmod 26 = 3$$

نتحصل على الحرف d.

3-1-8-تشفير بلافير Playfair cipher

هذه الشفرة تأخذ بلوك blockمكون من حرفين وأيضا الشفرة الناتجة تتكون من حرفين.

و طريقها تكون بعمل مصفوفة من 25 خانة(5×5)نضع في كل خانة حرف أبجديa و b وهكذا... وبالتالي نتحصل على حرف ليس له خانة، فنضع الحرفين i و j مع بعض في خانة واحد دائما.

و الجدول الآتي يوضح شكل المصفوفة:

a	b	C	d	e
f	g	H	i /j	k
l	m	N	o	p
q	r	S	t	u
v	w	X	y	z

الطريقة:

أولا ننظر إلى النص الأصلي و بالتحديد إلى كل بلوك مكون من حرفين، ونرى هل الحرفين متشابهين، إذا كان كذلك نفصل بينهما بالحرف x.

أيضا في حالة كان نهاية النص الأصلي بلوك مكون من حرف واحد نضيف له الحرف x، ثم ننظر إلى الجدول:

- إذاكان a و bكل منهما في عمود مختلف، نأخذ المربع الذي يمثل تقاطعهما (الحرفين الذين يمثلان نقطة تقاطع الصف مع العمود).
- إذاكان a و bفي نفس العمود، تشفير a هو الحرف الذي أسفله ذلك b.
- إذاكان a و b في نفس الصف، تشفير a هو الحرف الذي يمينه كذلك b.

مثال:

لدينا المصفوفة التالية معبئة بجملة التشفير:

l	o	v	e	i /j
s	a	m	n	y
p	d	r	t	h
g	b	c	f	k
q	u	w	x	z

نقوم بشفير النص التالي: ambassadorshot.

الحل:

- نقسم النص إلى بلوكات مكون من حرفين: ambass ad or sh ot .
- نفصل بين الحروف المتشابهة بالحرف x نتحصل على:

Am basxxs ad rs ho t

- لاحظ أن الحرف الأخير وحيد نضيف له الحرف xكالتالي:

Am basxxs ad rs ho tx

ننظر إلى الجدول، الحرف a في نفس صف الحرف m يتم ننتقل خطوة لليمين يكون حرف في البلوك الأول.

إذن تشفير a هو m و تشفير m هو n، وباقي البلوكات تشفر بنفس الطريقة وبالتالي نتحصل على النتيجة النهائية هي: Mn udqnambamp id fe.

فك التشفير:

و لفك التشفير العملية العكسية تصبح الذهاب إلى الخانةالأعلى في حالة وجود الحرفين في نفس العمود، و كذلك الذهاب إلى الخانة اليسرى في حالة وجود الحرفين في نفس الصف.

مثلا: نفك البلوكmn في نفس الجدول السابق.

m ترجع خطوة للوراء وتصبح a .

n ترجع خطوة للوراء وتصبح m.

3-1-9تشفير فيجينار cipherVigenére

$\mathbb{Z}_{26}^m = (\mathbb{Z}_{26})^m$ حيث $P = C = K = \mathbb{Z}_{26}^m$ و $m \in \mathbb{N}^*$.

$K = (k_1, k_2, \ldots, k_m)$ ذلك من أجل $k_i \in \mathbb{Z}_{26}$ و $1 \leq i \leq m$.

إذن:

$$E_k(x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m) = x + k$$

$$\mathcal{D}_k(y_1, \ldots, y_m) = (y_1 - k_1, \ldots, y_m - k_m) = y - k$$

مثال تطبيقي:

من أجل m = 3 و (4 , 11 , 2) = k الكلمة famille تشفر إلى hlqkwpg، حيث نقسم الكلمة إلى مجموعات كل مجموعة تحتوي على ثلاثة أحرف تكون متتالية، يشفر الحرف الأول بالمفتاح 2 و يشفر الحرف الثاني بالمفتاح 11 أما الحرف الثالث فيشفر بالمفتاح 4.

مثال:

المجموعة التي تحتوي على الأحرف famتشفر إلى hlq وذلك بتشفيرf الى hو a الى l وفي الأخير m الى q، نفس الشيء يطبق على بقية المجموعات.

ملاحظة:

يوجد أربعة أنواع لهذه الشفرة نذكرها:

1. شفرة فيجينار البسيطة.
2. شفرة فيجينار تلقائية المفتاح.
3. شفرة فيجينار طويلة المفتاح.
4. شفرة فيجينار الكاملة.

3-1-10-الشفرة الآمنة The one- time pad cipher

هذه الشفرة أكثر أمانا على مدى تاريخ التشفير، لم ولن يستطيع أحد كسر هذه الشفرة أبدا، إستخدمت هذه الشفرة في الكثير من الحكومات وأجهزة الإستخبارات.

الطريقة:

لدينا كتاب نطلق عليه one-time pad، بداخل هذا الكتاب توجد صفحات بداخل كل صفحة أرقام عشوائية لا تتكرر أبدا هذه الأرقام العشوائية تمثل الإزاحة المستخدمة (أي كل رقم منها هو مفتاح).

في حالة تم تشفير النص الأصلي بهذه الطريقة أقوم بإرسال النص المشفر و رقم الصفحة إلى الطرف الآخر، ثم اقطع الصفحة من الكتاب أي القضاء عليها، و الطرف الآخر يكون لديه نسخة مماثلة من الكتاب one-

time pad ويقوم بفك التشفير عن طريق رقم الصفحة، وبعدما يتم فك التشفير و الحصول على النص الأصلي يتم التخلص من الصفحة.

مثال:

لتكن لدينا الشفرة التالية: engage warp dive

و الصفحة الأولى تتكون من:

9 20 13 0 21 1 13 19 9 5 25 12 25 4 7 25 0 8 8 7 24 2 6 18 16 10 23 5 11 12

13 6 22 22 17 3 8 0 0 19 4 15

أقوم بجمع الحرف الأول e مع الرقم 9 لينتج n، وأجمع الحرف الثاني n مع الرقم 20 لينتج hو هكذا...

لينتج النص بعد التشفير كالتالي:Nhtabfjtauchve

ملاحظات:

1. إذا تبقت أرقام في الصفحة أو لم تبقى أقوم بتدمير الصفحة.
2. يستحيل كسر هذه الشفرة لأن المفتاح عشوائي لن يتكرر ابداً و في هذه الحالة لن يتم كسر الشفرة.
3. هذه الطريقة لا تستخدم هذه الأيام بسب صعوبة الاحتفاظ بهذا الكتاب و صعوبة إرساله إلى الطرف الآخر، أيضا صعوبة إضافة صفحات جديدة فيه.
4. لكن في حالة كنت مرسل الكتاب إلى الطرف الآخر من قبل، يمكنك إرسال شفرات بهذا النوع، ولن يكشفها أيّ أحد على الإطلاق إلا في حالة أنّ نكشف كتاب one-time pad .

الخاتمة

مما لاشك فيه ان للتشفير أهمية بالغةفي وقتنا الراهن حيث نعلم أن التشفير يستعمل في عدة ميادين فهو يعمل على حفظ سرية الرسائل.

وبكل بساطة يعتبر المنبع الاساسي لكثير من الشفرات الحديثة إضافة إلى أن دراستها تنمي العقل على التفكيرو يعزز روح البحث فيه، وبالتالي حاولنا في بحثنا هذا اعطاء مفهوم للتشفير وذكر بعضنماذج التشفير الكلاسكية التي ظهرت قديما موضحين الطرق المعتمدة في ذلك.

وقد ظهرت الآن طرق حديثة للتشفير يعتمد أساسا على التشفير الكلاسيكي ومازال هذا البحث متواصلا بتواصل تطور التشفير.

وفي الاخير نضع هذا العمل المتواضع و الذي لايخلو من النقائص أمام ايديكم ونرجو ان نكون قد وفقنا ولو بالقدر القليل في تخليد بصمة ضئيلة نوّد ان ندونها في صفحات البحث العلمي.

والله ولي التوفيق

المراجع

1. الزمر الدورية وانظمة التشفير، مذكرة التخرج لنيل شهادة استاذ التعليم الثانوي دفعة 2013.

2. الكتابة المشفرةمن إعداد طالب من طلاب كلية علوم الحاسب والمعلومات. جامعة الملك سعود.

3. مقدمة في التشفير بالطرق الكلاسكية، للكاتب وجدي عصام عبد الرحيم، 2007.

4. الكتاب االمدرسي السنة الثالثة ثانوي أدب و ثالثة رياضيات وتقني رياضي .

5. كتاب الرياضيات للديوان الوطني للتعليم عن بعد .

ملخص

من خلال هذا البحث حاولنا إعطاء مفهوم للتشفير ودراسة أهم أنظمة التشفير الكلاسيكية معتمدين في ذلك كل مايتعلق بالموافقات و القسمة في $\mathbb{Z}$ من خواص وتعاريف ...إلخ كما قمنا بعرض الطرق المتبعة في أهم نماذج التشفير مع الدعم بأمثلة توضيحية.

في الأخير نرجو أننا قد أصبنا ولو بالجزء القليل من مبتغانا في بحثنا هذا كما نسال الله عزّ وجل أن يعود بهذا العمل علينا وعلى كافة الطلبة بالنفع والفائدة.

الكلمات المفتاحية:

التشفير، فك الشفير، أنظمة الشفير الكلاسيكية، الموافقات في $\mathbb{Z}$ ، القسمة الاقليدية

Abstract

We tried through this research to explain the concept of encryption, and to study the most important classical encryption systems relying on all what matters concerning approvals and division in $\mathbb{Z}$ such as properties, difinitions, and so on. In addition, we have presented the methods used in the most significant encryption models supporting it with illustrative examples.

Key words :

Cryption, cipher, decryption, classical encryption systems, approvals in $\mathbb{Z}$

Résumé

A travers ce projet nous avons essayé de donner un concept pour la cryptographie et étudier les importants systèmes de cryptographie classique, reposant dans notre étude sur tous ce qui concerne les approbations et la division dans $\mathbb{Z}$ des propriétés et définitions … etc.

Nous avons aussi présenté les méthodes suivis dans les plus importants modèles de cryptage avec l'assistance des exemples explicatifs.

Enfin, nous espérons atteindre même une petite partie de notre objectif de cette étude comme nous prions dieu tout-puissant que ce projet retourne sur nous et tous les étudiants par le bénéfice et l'intérêt.

Mots clés

Cryptographie, décryptographie, système de cryptographie classique, approbations en$\mathbb{Z}$ division euclidienne.